

HCBS Remote Monitoring Requirements

Remote monitoring (RM) is defined as the use of communication and non-invasive monitoring technologies to assist participants on the Comprehensive and Supports Waiver to attain or maintain independence in their homes while minimizing the need for onsite staff presence and intervention.

Participants receiving Medicaid home and community-based services funded by the Comprehensive or Supports Waiver programs may be offered, where appropriate, the opportunity to be served through the use of an electronic RM system as a component of Community Living Services (CLS).

Wyoming RM systems must be designed and implemented to promote the health and welfare of the participant in their own home, while maintaining the highest level of privacy. Furthermore, the system must be monitored by an individual trained and oriented to the specific needs of each participant served as outlined in the participant's individualized plan of care (IPC).

RM is an element of CLS and is not a stand-alone service. The use of RM must be outlined in an individualized RM protocol, fit within the scope and definition of the CLS tier being received, and adequately support the supervision needs of the participant. Although the intent of remote monitoring is to decrease participant dependence of on-site staff presence, it is not intended to replace provider presence during times the participant needs in-person support or supervision. Some level of in-person interaction during each 24 hour period.

REQUIREMENTS

A. Definitions

- i. "Backup procedures" are defined as written procedures that outline the provider response in the event that remote monitoring systems fail or additional personnel are needed.
- ii. "Backup system" is defined as a system designed to engage in the event that there is a failure in remote monitoring technology, including but not limited to power failure, communication failure, or sensor malfunction.
- iii. "Monitoring base" is defined as the location from which the remote monitoring staff monitors a participant.
- iv. "Remote Monitoring Risk Assessment" is defined as a systematic process and resulting document used by the plan of care team to evaluate the potential risks that may be involved in remote monitoring, and identify ways in which identified risk can be mitigated through technology.
- v. "Sensor" is defined as the equipment used to notify the remote monitoring staff or other individuals designated in the IPC, of a situation that requires attention or activity at the residence that may indicate future needs or deviations from routine activity. Examples include, but are not limited to door sensors, motion detectors, heat detectors, and smoke detectors.

B. Availability

- i. Participants 18 years or older, or the participant's legally authorized representative, may request supervision through RM.
- ii. RM is only available to participants receiving a CLS tier of Basic Daily Level 3 or Level 4. Participants receiving Basic 15 minute units are presumed to have significant time without staff, and any technology used is considered to be a support. This support must be written into the IPC, but does not meet the criteria for RM. CLS Levels 5 and 6 shall not be reimbursed if RM services are provided.

C. Assessment and Informed Consent

- i. The participant must be preliminarily assessed by the plan of care team, using the Division required Remote Monitoring Risk Assessment form. The form must include the approval and signature of the legally authorized representative, if applicable, and must be maintained in EMWS and included as part of the IPC.
- ii. The completed assessment must be discussed, and all identified health and safety concerns must be addressed, prior to utilizing RM. This discussion must include full participation of the plan of care team.
- iii. Initially, the plan of care team must assess and determine that continued usage of the RM system will facilitate the health and welfare of the participant at the three month and six month milestone. After the first six months, the plan of care team must assess the appropriateness of continued usage at least every six months. A review of the risk assessment, RM protocol, and all incident reports and other relevant documentation, to include alert, response, and staff response logs, must be part of these assessments. Team notes, updated RM protocols, and updated Risk Assessments must be uploaded in EMWS.
- iv. An informed consent statement must be signed by the participant and legally authorized representative. The form must include confirmation that the participant had a choice between in-person and remote monitoring, acknowledgement of the inherent risk associated with remote monitoring, indication that they have been adequately informed of the operating parameters and limitations of the service delivery model, and agreement to the protocol developed by the team. A copy of the informed consent form must be maintained in EMWS and in the participant's individual file, and an updated informed consent form must be obtained annually.
- v. Updated informed consent forms must be obtained annually.
- vi. The plan of care team must identify other participants in the setting who may be affected by the remote monitoring, and obtain informed consent from each of these individuals. This consent, and any rights restrictions that may result from the housemate's use of remote monitoring, must be documented in each participant's IPC.

D. Remote Monitoring Protocol Guidelines

The plan of care team must develop an individualized RM protocol for each participant receiving RM. The RM protocol must be uploaded in EMWS as part of the IPC. The RM protocol is intended to be a guiding document for the plan of care team and remote monitoring staff, and

must outline how remote monitoring will be implemented for each participant. The RM protocol must include:

- i. The specific technologies that will be utilized, and what each of these technologies will monitor.
- ii. Supervision needs identified through the risk assessment (i.e.; kitchen, community, personal care, medication), and how these needs will be addressed through technology.
- iii. Results of ongoing assessment to assure remote monitoring continues to be an appropriate option for the participant.
- iv. Response mechanisms and timeframes for each alert/alarm/notification.
- v. Information related to how the provider should support the participant in the event of a system failure, outage, or disengagement.
- vi. If applicable, de-escalation techniques unique to remote monitoring services, and potential elopement locations.
- vii. Backup procedures for the specific location in which the participant resides.
- viii. Staff response time at the participant's living site from the time the needed support is identified and acknowledged by the RM staff. The RM staff must be able to explain any extenuating circumstances, and these circumstances must be verifiable by the Division.

E. Case Manager Guidelines

- i. During monthly home visits, the case manager must review provider adherence to all remote monitoring standards and protocols. They must discuss concerns the participant has with their remote monitoring technology, and follow up with the provider to ensure the concerns are addressed.
- ii. The case manager must ensure all required review and follow up meetings are scheduled, conducted, and documented.
- iii. The case manager must update the IPC and ensure that all documents related to RM are current and stored in EMWS. In order to accurately identify the participant as utilizing RM, the case manager must:
 - a. On the Circle of Supports screen, under the *Housing* tab, select that remote monitoring is used;
 - b. On the Needs and Risks screen, above the list of support areas, answer *Yes* to the question "Does this plan include remote support?"
 - c. Upload the following documents on the Needs and Risks screen:
 - i. Remote Monitoring Risk Assessment
 - ii. RM protocol
 - iii. Team notes and other relevant documentation

F. Remote Monitoring Devices

Remote monitoring devices will belong to the participant, and may be paid through Specialized Equipment Services, as long as the equipment meets the participant's needs as indicated in the participant's Remote Monitoring Risk Assessment. The devices must meet the service definition, cannot exceed the Specialized Equipment Services cap, and must fit within the participant's

individual budget amount (IBA). Continuous live audio/video feed and recorded audio/video feed are not acceptable forms of remote support.

The following device categories will be authorized for remote monitoring:

- i. Door, motion, stove, and bed sensors
- ii. Panic buttons and pendants
- iii. Fire/carbon monoxide alerts and monitoring - Can the state please specify in the service definition if fire/carbon monoxide detection will include monitoring and how? This category is specific to devices that will send notification to a remote monitor when triggered and does not include typical fire and carbon monoxide detectors.
- iv. Strobe lighting for visual alerts
- v. Assistive technology such as calendars and alarms
- vi. Staff check-in buttons
- vii. Cues to prompt independence, such as recorded reminders when a participant enters or exits a room.
- viii. Smart thermostats, lightbulbs, door openers, automated door locks, outlet switches, and mechanical faceplate light switches
- ix. Doorbell integration
- x. 24/7 Response Center option

G. Operating Guidelines

- i. Remote monitoring can only be offered by a provider organization that is composed of two or more staff members.
- ii. At the RM base, the provider must maintain a file on each participant monitored. The file must include a current photograph of each participant, which must be updated if significant physical changes occur, and at least annually. The file must also include pertinent information on each participant, noting facts that would aid in facilitating the participant's safety. All files must be maintained and accessed in a way that assures ongoing HIPAA compliance.
- iii. The provider must have backup procedures for system failure (e.g., prolonged power or internet outage), fire or weather emergency, participant medical issues, or personnel emergency in place and detailed in writing for each site utilizing the system, as well as in each participant's RM protocol. This plan must specify the staff position(s) to be contacted, and who will be responsible for responding to these situations and traveling to the remote living site(s), if necessary.
- iv. Monitoring must be conducted in real time. Monitoring via audio or video recording is not allowable.
- v. While remote monitoring is being provided, the RM staff must not have duties that will impose on RM responsibilities in any way.
- vi. Provider must ensure that RM staffing is adequate to respond to all alerts and emergencies for all participants receiving RM, as identified in each participant's IPC, and as outlined in Chapter 45, Section 6 of the Wyoming Medicaid rules. Response could include, but is not limited to: phone calls, text messaging, webcam applications, and on-site visits, and must be specifically addressed in the individualized RM protocol.

- vii. Additional staff must assist the participant in the home as needed to ensure the urgent need or issue that generated a response has been resolved. If needed, relief staff must be made available by the provider. Coverage strategies must be available to the Division upon request.
- viii. RM equipment must include a visual indicator to the participant that the system is on and operating.
- ix. The participant must have full control of the remote monitoring devices. A mechanism to disengage the RM system at the participant living site must be in place. If the system is disengaged during the agreed service span without consultation or prior agreement, this constitutes an internal incident. If the participant chooses to disengage the system, the provider must ensure appropriate on-site staff support.
- x. Emergency response drills must be conducted, documented, and be available for review as required by Division standards and rules. At least one on-site response drill must be conducted for each participant annually.
- xi. Staff response time to the participant's living site from the time the needed support is identified and acknowledged by the RM staff must be addressed in the RM protocol. The RM staff must be able to explain any extenuating circumstances, and these circumstances must be verifiable by the Division.
- xii. Appropriate communication and 911 emergency responses must be determined through the Remote Monitoring Risk Assessment, approved by the plan of care team, and documented in the IPC and RM protocol.
- xiii. If a provider uses an outside entity to address the technology used in remote monitoring, the technology agency will not be required to be a Wyoming provider. However, if an entity used by the CLS provider has any interaction with the participant (i.e., in person response, phone calls, Skype or Facetime), then that entity is providing CLS and will be required to meet rules established in Chapter 45, either as a Wyoming provider, provider employee, or subcontractor.
- xiv. The use of the remote monitoring option must not block, prohibit or discourage the use of in-person services or access to the community.
- xv. A participant who requires in-person assistance during the provision of the service must receive services in-person.
- xvi. Remote monitoring cannot be used for the provider's convenience. The option can only be used to support a participant to reach identified outcomes in the participant's individualized plan of care. In the event the participant or legally authorized representatives chooses to discontinue remote monitoring services, the provider and plan of care team must transition the participant to traditional services within 30 calendar days.

H. Provider Standards

Providers offering remote monitoring opportunities must meet all federal, state, and local regulations, including the registration of equipment, if applicable. Additionally, providers must meet the following standards and receive written authorization from the Division to provide remote monitoring. These standards are subject to change. Providers shall receive notification of changes to standards, and are required to adhere to changes within thirty (30) calendar days of notification.

- i. Written policies that assure the participant's right to privacy.
- ii. Use of a HIPAA-compliant telehealth service delivery platform approved by the Division. During the provider certification renewal process, providers that deliver remote monitoring services must sign an attestation that indicates:
 - They are using a HIPAA-compliant platform; and
 - They have adopted and enforced all necessary policy and procedures under the HIPAA Privacy & Security Rules.

At all times, the Division may review a provider's compliance in this regard. If a provider is found to not use the HIPAA-compliant platform or to not have adopted or enforced necessary policies and procedures, the Division may prohibit or restrict each provider's ability to provide remote monitoring.

- iii. Providers must receive training on participant specific needs, including the support the participant will need in order to learn and utilize remote monitoring technologies. Providers must develop and implement a policy that describes how they will support initial and ongoing participant training in areas that include, but are not limited to, emergency drills, remote monitoring equipment, disengaging the system, and responding to system failure. Provider policies shall be approved by the Division before they will be certified to provide remote monitoring services.
- iv. Providers will be ultimately responsible for the remote monitoring activity. All monitoring must be conducted in real time and provided by an individual who is awake. As identified in the corresponding service tier, on-call 24 hour support or a contingency plan for emergency situations must be outlined in the participant's IPC. The provider must be available to respond as outlined in the participant's remote support protocol, which may include in-person response within specific time-frames.
- v. System backup procedures.
- vi. Emergency response drills, including one on-site response drill every twelve (12) months.
- vii. Staffing strategy that demonstrates how all participants receiving remote monitoring will receive necessary responses as outlined in the RM protocol and IPC.
- viii. Policy covering initial and ongoing participant training, which includes, but is not limited to, emergency drills, RM equipment, disengaging the system, and responding to system failure.
- ix. Policy covering initial and ongoing RM staff training, which includes, but is not limited to, participant RM protocols, emergency drills, RM equipment, response requirements, HIPAA compliance and other trainings identified in Chapter 45 of Wyoming Medicaid Rules, and policies and procedures related to remote monitoring.
- x. Updated cost disclosure policy that includes participant and organizational costs for remote monitoring equipment and services (internet, phone line).
- xi. Policy addressing a participant's immediate transition from RM services should a health or safety need be identified that overrides the 30 calendar day transition timeline.
- xii. Response procedure for participant disengagement of the system.
- xiii. Procedure for notification of emergency response personnel (i.e., law enforcement, fire, paramedic).
- xiv. Emergency procedures for weather related and medical emergencies.
- xv. Documentation of HIPAA privacy and security compliance.
- xvi. Updated contingency plan that includes remote monitoring services.

I. Documentation

- i. As required in Chapter 45, Section 20 of Wyoming Medicaid Rules, critical incident reports must be submitted through the Division's incident reporting system.
- ii. Alert notifications, responses, and staff interventions required during the RM period must be documented as an internal incident, and reviewed as a component of the ongoing plan of care team assessment. If these situations become excessive, the team should reconvene to review incident reports. If RM is still determined to be an appropriate support, the plan of care team may develop a system to track the specific notification/response/staff intervention without completing an incident report.
- iii. RM information must be retained for at least six (6) years after the end of the fiscal year during which services were provided.

J. Reimbursement for Services

- i. RM is a component of CLS, and is covered through the service rate identified in the current Supports and Comprehensive Waiver Fee Schedule. In-person interaction during each 24 hour period is required in order for the provider to be reimbursed for CLS.
- ii. Providers shall not be reimbursed for their expenses related to internet, communications, monthly subscriptions, or other expenses considered to be a cost of doing business. Business expenses incurred by the provider, as a result of providing RM, cannot be passed on to the participant.
- iii. Equipment that is specific to a participant may be purchased through specialized equipment. Equipment will be subject to the scope and limitations of this service.
- iv. Equipment purchased under specialized equipment will be the property of the participant.
- v. Equipment purchased under specialized equipment must fit within current funding guidelines as outlined in the current Comprehensive and Supports Waiver Service Index.

K. Best Practices

- i. Assure confidentiality through the use of a headset, soundproofing, screen protector, etc.
- ii. Establish communication between shifts or services, through written logs or other documentation, to assure all providers have the information necessary to provide seamless transitions between services and staff members.
- iii. Encourage participants to purchase renters insurance, which covers personal belongings and technology or systems necessary to provide remote monitoring.
- iv. Take advantage of incidental learning situations to discuss safety in the home and community.